PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0
Internet: http://www.fcc.
TTY: 1-888-835-5

DA 05-387
February 11, 2005

DOMESTIC AUTHORIZATION GRANTED

APPLICATION OF INFONET BROADBAND SERVICES CORPORATION AND INFONET TELECOMMUNICATIONS CORPORATION TO TRANSFER CONTROL OF FCC LICENSES AND AUTHORIZATIONS TO BT GROUP PLC

WC Docket No. 04-421

By the Chief, Wireline Competition Bureau:

On November 19, 2004, Infonet Services Corp. ("Infonet") and BT Group plc ("BT Group") (together, the "Applicants") filed an application pursuant to sections 63.03 and 63.04 of the Commission's rules[1] requesting approval to transfer control of Infonet Telecommunications Corporation ("ITC") from Infonet to BT Group.[2] BT Group is a widely-held public corporation and holding company organized under the laws of England and Wales.[3] Upon consummation of the transaction giving rise to the transfer of control, ITC will be wholly-owned by BT United States L.L.C., a Delaware limited liability company that is indirectly wholly-owned and controlled by BT Group.[4]

The Commission released a public notice accepting this application for streamlined processing on November 30, 2004.[5] Subsequently, on December 14, 2004, the Applicants, along with the United States

1 47 C.F.R §§ 63.03, 63.04; *see* 47 U.S.C. § 214.

2 Applicants also filed for transfer of control related to international section 214 authority held by ITC's affiliate, Infonet Broadband Services Corporation ("IBSC"), as well as an Infonet wireless license, both of which are part of this same transaction.

3 No person or entity owns 10 percent or more of the equity of BT Group. *See* Letter from Yaron Dori, Counsel for Applicants, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 04-421, (November 24, 2004) at 1.

4 The vertical ownership structure between BT United States L.L.C. and BT Group is through multiple BT affiliates, each of which is organized under the laws of England and Wales. Specifically, BT United States L.L.C. is 100% owned by BT Fifty-Three Limited. BT Fifty-Three Limited is, in turn, owned by BT Fifty-One, Limited (33%) and BT (International) Holdings Limited, (67%), both of which are 100% owned by BT Holdings Limited. BT Holdings Limited is wholly owned by British Telecommunications plc ("BT"), which is, in turn, 100% owned by BT Group Investments Limited. BT Group Investments Limited is wholly-owned by BT Group.

5 *Domestic Section 214 Application Filed for Transfer of Control of Infonet Broadband Services Corporation and Infonet Telecommunications Corporation to BT Group plc*, WC 04-421, Public Notice, DA 04-3791 (rel. Nov. 30, 2004).

Department of Justice ("DOJ"), including the Federal Bureau of Investigation ("FBI") on behalf of the United States Department of Homeland Security ("DHS") (collectively, the "Executive Branch Agencies"), filed with the Commission a joint petition to defer grant of this application while the Executive Branch Agencies and Applicants addressed potential national security, law enforcement, and public safety issues.[6] On February 2, 2005, the Executive Branch Agencies submitted a Petition to Adopt Conditions to Authorizations and Licenses ("Petition").[7] In the Petition, the Executive Branch Agencies advised the Commission that they do not object to the grant of the instant application, provided that the Commission conditions such grant on compliance by BT Group with the commitments and undertakings made in a January 12, 2005 letter to the Executive Branch Agencies (the "BT Infonet Commitment Letter"),[8] a copy of which was attached to the Petition. Applicants have not objected to the Petition.[9]

Consistent with Commission precedent, the Bureau accords the appropriate level of deference to the Executive Branch Agencies' expertise on national security and law enforcement issues.[10] The Executive Branch Agencies indicate that the commitments set forth in the BT Infonet Commitment Letter address their stated concerns regarding national security, law enforcement, and public safety.[11]

The Wireline Competition Bureau finds, upon consideration of the record, that grant of the Application, subject to the condition set forth in this Public Notice, will serve the public interest, convenience, and necessity.[12] Specifically, in accordance with the request of the Executive Branch

---

6 *See* Application Pursuant to Section 214 of the Communications Act of 1934 and Section 63.04 of the Commission's Rules for Consent to the Transfer of Control of Infonet Telecommunications Corp. to BT Group, plc, WC Docket No. 04-421, Joint Petition to Defer (filed Dec. 14, 2004) (Joint Petition to Defer).

7 Department of Justice, Federal Bureau of Investigation, and Department of Homeland Security, Petition to Adopt Conditions to Authorizations and Licenses, WC Docket No. 04-421 (dated Jan. 31, 2005) ("Petition").

8 Letter from Tim Cowen, General Counsel. Global Services, British Telecommunications plc, to Laura H. Parsky, Deputy Assistant Attorney General, United States Department of Justice, Tina W. Gabbrielli, Director of Intelligence Coordination and Special Infrastructure Protection Programs, United States Department of Homeland Security, and Patrick W. Kelley, Deputy General Counsel, Federal Bureau of Investigation (dated Jan. 12, 2005). This letter is attached to this Public Notice as Appendix A.

9 Moreover, the Executive Branch Agencies indicate they are authorized to state that the Applicants do not object to grant of the Petition. *See* Petition at 4.

10 The Commission considers national security, law enforcement, foreign policy, and trade policy concerns when analyzing a transfer of control or assignment application in which foreign ownership is an issue. *See Amendment of the Commission's Regulatory Policies to Allow Non-U.S. Licensed Satellites Providing Domestic and International Service in the United States*, Report and Order, 12 FCC Rcd 24094, 24170-72, ¶¶ 178-182 (1997) ("*DISCO II Order*"); *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23919-921, ¶¶ 61-66 (1997), Order on Reconsideration, 15 FCC Rcd 18158 (2000) ("*Foreign Participation Order*"). In assessing the public interest, the Commission considers the record and accords the appropriate level of deference to Executive Branch expertise on national security and law enforcement issues. *See Foreign Participation Order*, 12 FCC Rcd at 23919-921, ¶¶ 61-66; *see also Applications of XO Communications, Inc. for Consent to Transfer Control of Licenses and Authorizations Pursuant to Sections 214 and 310(d) of the Communications Act, and Petition for Declaratory Ruling Pursuant to Section 310(b)(4) of the Communications Act*, IB Docket No. 02-50, Memorandum Opinion & Order, 17 FCC Rcd 19212, 19228-29, ¶¶ 36-40.

11 *See* Petition at 3.

12 *See* 47 C.F.R. § 63.03(c)(v). Upon consummation of the transaction, BT Group will have a market share in the U.S. interstate interexchange market of less than 10 percent, and will provide competitive telephone exchange services or exchange access services exclusively in geographic areas served by a dominant local exchange carrier in

Agencies, in the absence of any objection from the Applicants, pursuant to section 214 of the Communications Act of 1934, as amended, 47 U.S.C. § 214, and section 0.291 of the Commission's rules,[13] the Wireline Competition Bureau hereby grants this Application conditioned on compliance with the commitments set forth in the BT Infonet Commitment Letter, which is attached hereto as Appendix A.

Pursuant to section 1.103 of the Commission's rules, the grant is effective upon release of this Public Notice.[14] Petitions for reconsideration under section 1.106 or applications for review under section 1.115 of the Commission's rules may be filed within 30 days of the date of this Public Notice.[15]

For further information, please contact Alex Johns at (202) 418-1167, or Terri Natoli at (202) 418-1574, Competition Policy Division, Wireline Competition Bureau.

– FCC –

---

the U.S. that is not a party to the transaction. In addition, no party to this transaction is dominant with respect to any domestic service.

[13] 47 C.F.R. § 0.291.

[14] *See* 47 C.F.R. § 1.103.

[15] *See* 47 C.F.R. §§ 1.106, 1.115.

Appendix A

Infonet Commitment Letter

January 12, 2005

BY HAND DELIVERY

Ms. Laura H. Parsky
Deputy Assistant Attorney General
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Ms. Tina W. Gabbrielli
Director of Intelligence Coordination and
Special Infrastructure Protection Programs
United States Department of Homeland Security
Washington, D.C. 20528

Mr. Patrick W. Kelley
Deputy General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Ms. Parsky, Ms. Gabbrielli and Mr. Kelley:

As you know, British Telecommunications plc ("BT"), a United Kingdom company engaged in the provision of global communications services and solutions, plans to acquire Infonet Services Corporation ("Infonet"), a Delaware corporation offering value-added network communications services.

BT and Infonet have met with representatives of the U.S. Department of Justice ("DOJ"), including the Federal Bureau of Investigation ("FBI"), and the U.S. Department of Homeland Security ("DHS") to discuss BT's security arrangements with respect to the planned transaction. Further to those discussions, this letter now sets forth certain security assurances of BT to the DOJ, FBI and DHS in connection with BT's acquisition of Infonet. These security assurances relate to the combined network facilities of BT and Infonet physically located in the United States ("BT U.S. Facilities") and will be effective immediately upon consummation of the acquisition of Infonet by BT.

Specifically, following consummation of the transaction, BT will maintain security policies designed to protect BT U.S. Facilities, safeguard U.S. Customer Data, as hereinafter defined, respond to security incidents, and comply with U.S. law enforcement requests. In furtherance of the foregoing security objectives, BT undertakes the following:

British Telecommunications plc
Registered Office
81 Newgate Street, London EC1A 7AJ
Registered in England no. 1800000
BT is an ISO 9001 Registered Company

www.bt.com

Maintenance of U.S. Security Policy and Operational Plan. BT will maintain a security policy and operational plan for the BT U.S. Facilities (the "Security Policy"), including all of the elements set forth below. The Security Policy will address BT's broad security objectives with respect to its U.S. Facilities as well as specific standards and practices to be applied in the BT organization including, but not limited to, facility access, security management, employee screening, cooperation with U.S. law enforcement and related matters.

Designation of U.S. Security Committee. BT will designate at least two (2) persons to serve as members of a security committee (the "Security Committee"). BT contemplates that the Security Committee initially will be comprised of four persons: (i) the BT Americas General Counsel; (ii) the Head of U.S. Network Operations; (iii) the U.S. Security Officer; and (iv) the U.S. Law Enforcement Primary Contact Person. BT expects that the composition and number of members of the Security Committee may change from time to time, but in any event will have a minimum of two members, one of which will be the BT Americas General Counsel and one of which will be the Head of U.S. Network Operations. The Security Committee will meet periodically (no less than quarterly) to review the Security Policy and confirm that BT is in operational compliance with the Security Policy. The Security Committee will be responsible for ensuring that the Security Policy is followed in the event of a high level threat or national emergency in the United States. The Security Committee will also be responsible for making appropriate revisions to the Security Policy as needed in light of changes and modifications to the BT global network. The members of the Security Committee will be resident U.S. citizens and will be subject to the third-party, pre-employment screening process at the higher level described below.

3. **Designation of U.S. Security Officer**. BT will designate a Security Officer for the BT U.S. Facilities. The Security Officer will oversee the day-to-day implementation and maintenance of the Security Policy for the BT U.S. Facilities. The Security Officer will report to the Security Committee. The Security Officer will be a resident U.S. citizen and will be subject to the pre-employment screening process at the higher level described below.

Designation of U.S. Network Security Response Team. BT will designate a U.S. Network Security Response Team to support and manage BT's U.S. Facilities. The U.S. Network Security Response Team will consist of key personnel from across BT Americas and will have the primary responsibility of assuming ultimate control of BT U.S. Facilities in the event of a high level threat or U.S. national emergency, including (i) terminating control of U.S. Facilities by persons outside the United States; (ii) performing network changes as required, and (iii) maintaining functions to minimize the impact of such threat or emergency to BT's customers. For purposes of the foregoing, to "assume control" in this context means to take necessary action to prohibit personnel physically located outside the United States from performing activities directly related to the physical operation of BT's U.S. Facilities, including but not limited to surveillance, maintenance, integration, commissioning and network management functions.

5. **Compliance with U.S. Law Enforcement Requests**. BT will maintain policies and procedures for the provision of, or for providing access to, within the United States, electronic or wire communications (whether stored or real-time), subscriber information, billing and transactional records of U.S. subscribers (the "U.S. Customer Data") requested by U.S. law enforcement agencies, either pursuant to lawful U.S. process or as otherwise permitted by law. BT will designate one or more points of contact at an office within the United States to receive and process, in a secure and efficient manner, requests for assistance from U.S. law enforcement agencies, including requests for interception or surveillance of communications and compliance with subpoenas or other lawful demands for disclosure of, or access to, BT's records. Such assistance will include, but not be limited to, disclosure, if necessary, of technical and engineering information relating to the design, maintenance or operation of BT's systems. BT and the law enforcement agency seeking the assistance will work together to determine what assistance is reasonable, taking into account the investigative needs of the agency and BT's commercial interests. BT will designate a screened technical official to assist, where applicable, in execution of such requests for assistance from law enforcement agencies. BT also will provide for the confidential treatment, and prohibition of unauthorized disclosure, of the record of such requests and all information supplied to law enforcement in response to such requests. Upon designation, BT will notify the FBI, DOJ and DHS in writing of the points of contact, and thereafter will promptly notify the FBI, DOJ and DHS of any change in such designation. The points of contact will be resident U.S. citizens and will be subject to the pre-employment screening process at the higher level described below.

6. **Maintenance of Access Control Policy**. BT will maintain an access control policy (the "Access Control Policy"), which policy will include access control requirements for BT's U.S. Facilities. The Access Control Policy will require in particular that all BT U.S. Facilities be secured and that, while on the premises of BT U.S. Facilities, all employees and visitors must display appropriate identification. The Access Control Policy will also provide that approved visitors are escorted by a BT employee at such times that said visitor has access to U.S. communications or network infrastructure. The minimum requirements for access by any person to any BT U.S. Facility will be that the person (i) is an employee and is based in that particular facility; or (ii) is an expected visitor and has made arrangements for entry with a BT employee host.

7. **Requirement of Unique User Identification**. BT's Access Control Policy will require that each user of computer systems associated with BT's U.S. Facilities be assigned a unique user ID and password for purposes of accessing such systems. Further, access will be granted solely on an "as needed" basis, with individuals obtaining access exclusively to the systems needed to perform their specific job obligations.

8. **Network Monitoring**. BT will monitor its U.S. Facilities in order to detect and prevent malicious access attempts, as well as to resolve technical faults and potential security vulnerabilities. U.S. resident personnel will control the U.S. portions of BT's network with respect to integration, commissioning, and implementation of network

and customer equipment, bandwidth activations, node site management and technical assistance. U.S.-resident personnel will also maintain the ability to assume control over the U.S. portions of the network, including the ability to terminate control by personnel located outside of the U.S. in the event of a high level threat or national emergency.

9. **Maintenance of Screening and Non-Disclosure Requirements**. BT will require pre-employment screening and non-disclosure commitments prior to hiring new employees with access to the BT U.S. Facilities. Higher-level screening will be mandatory for officers of BT and those individuals who already hold, or will hold, particularly sensitive network positions ("Sensitive Network Personnel"), including the members of the Security Committee, the Security Officer, the U.S. Network Security Response Team and the technical official referenced in Paragraph 5 above. The list of positions designated as Sensitive Network Personnel will be reviewed periodically by the Security Officer and approved by the Security Committee to ensure that the appropriate persons are so designated and have been properly screened according to the Security Policy. Prior to such approval, BT will provide DOJ, FBI, and DHS a two week comment period to review the initial list of Sensitive Network Personnel positions and to provide input into the required level of screening for certain sensitive positions. BT will promptly notify DOJ, FBI and DHS of any material changes made in the list thereafter.

10. **Protection of U.S. Customer Data**. BT's Security Policy will include appropriate policies and procedures, consistent with BT's compliance with U.S. and foreign laws, to protect U.S. Customer Data from unauthorized access and from mandatory destruction under any foreign laws, and to require prior consent of the DOJ, FBI and DHS before disclosing U.S. Customer Data to non-U.S. persons who are not screened, consistent with BT's Security Policy, to a level commensurate with the sensitivity of the data to which they have access. Such prior consent is not required for compulsory disclosure pursuant to valid legal process enforceable by a non-U.S. government, in which case BT will give prompt notice to DOJ, FBI and DHS, of the service upon BT of any such process so long as such notice to DOJ, FBI and DHS is not in violation of foreign law. Should any non-U.S. person have access to the content of communications, they would be screened to a substantively identical level as would Sensitive Network Personnel, consistent with the law of the jurisdiction governing such screening. Unauthorized disclosure of U.S. Customer Data will be required to be reported promptly to the Security Committee, which will investigate the matter and make referrals to U.S. law enforcement when it reasonably appears that U.S. law may have been violated, with a copy of any such referral to DOJ, FBI and DHS. BT's policies regulating the disclosure of U.S. Customer Data will also apply to agents and contractors of BT through non-disclosure agreements, as appropriate.

11. **Reporting of Network Changes**. BT's Security Policy will require that any major acquisitions, modifications, upgrades or changes made to BT's U.S. Facilities, including network operating systems, software and access security be promptly reported to the Security Officer and the Head of U.S. Network Operations.

12. **Reporting of Security Breaches.** BT's Security Policy will require that all breaches and suspected breaches of network security that directly and significantly impact the operations or overall management of BT's U.S. Facilities will be promptly reported to the Security Committee. The Security Policy will further require that such matters be investigated by the BT Americas General Counsel and the Security Officer, and that referrals be made to U.S. law enforcement when it reasonably appears that U.S. law may have been violated, with a copy of any such referral to DOJ, FBI and DHS. BT's Security Policy also will require that the Security Officer maintain a record of such actual or suspected breaches. DOJ, FBI and DHS will have a right, with two weeks notice to BT Americas General Counsel and the Security Officer, to inspect the record of reports of all breaches and suspected breaches to the Security Committee, and to obtain on request a brief report of investigation in any matter of concern.

* • •

The assurances provided in this letter reflect BT's commitment to maintaining secure facilities in the United States, as well as BT's desire to continue its strong working relationship with the United States government. Should there be any material changes with respect to BT's security arrangements, or in the facts and circumstances set forth in this letter, or in the letter of November 18, 2004, to DOJ, FBI, DHS, and other U.S. Government agencies, BT will promptly notify DOJ, FBI, and DHS. Should you have any questions regarding any aspect of this letter, please do not hesitate to contact the undersigned.

Very truly yours,

British Telecommunications plc

Date: 12/01/05

By: [signature]

Printed Name: TIM COWEN
Title: GENERAL COUNSEL
GLOBAL SERVICES